## REMARKS

### I. INTRODUCTION

Claims 1-25 are pending in the present application, and claim 15 has been amended to cure a punctuation error. No new matter has been added. In view of the above amendments and following remarks, it is respectfully submitted that all of the presently pending claims are allowable.

### II. THE 35 U.S.C. § 102(b) REJECTIONS SHOULD BE WITHDRAWN

The Examiner has rejected claims 1, 6-8, 10, 11, 14, 15, 18-20, 22, and 23 under 35 U.S.C. § 102(b) as unpatentable over U.S. Patent No. 5,021,779 to Bisak. (hereinafter "Bisak")

Bisak is directed toward a system for providing a security device for an electrical appliance that derives input from an electrically connected external source. The external source is physically separate from the appliance and electrically connected, meaning physically connected, through conducting means, not wirelessly through air medium. The system is designed to secure an appliance by requiring a predetermined code to be entered for normal operation. The code comes from an electrically connected encoder. If the appliance does not receive the correct code then the unit is rendered inoperable, and an alarm is transmitted over the electrical wiring to a specified destination. (See Bisak, col. 1, line 35 – col. 2, line 26).

Claim 1 recites an "a wireless transmitter (20) for the equipment for broadcasting a beacon signal indicating stolen status, if the lock does not receive a valid key." The Examiner asserts that this recitation of claim 1 is disclosed in Bisak at column 4, lines 42-60. (See 4/5/07 Office Action, pp. 2-3). Applicants respectfully disagree. This passage from Bisak states,

> In one mode, upon no signal being received due to unplugging the appliance, unplugging the transmitter, or if the wrong code is received, the decoders output will go high thereby sounding an audio alarm 32 inside the appliance. Also, if the appliance is plugged in at a place remote from the transmitter (assume appliance has been stolen) it will not operate without the correct

> code being received.
>
> In another mode, upon removing appliance from wall socket or from its power source, the output of the decoder 30 would energize a device 33 which would trigger an external alarm. For example, it may trigger the external alarm through a radio link or some other method. A small transmitter inside the appliance (not to be confused with the transmitter-encoder) may be used and an external receiver which would pick up the signal from the transmitter, upon which it would set off an external alarm (silent or other) for example phone dialler.

However, Applicants submit that a beacon signal indicating stolen status if the lock does not receive a valid key is different from the external alarm triggered through a radio link as stated in Bisak.

Bisak describes two modes related to the security device. In the first mode, an alarm located on the appliance, is sounded when the appliance is unplugged, the transmitter is unplugged, or if the wrong code is received. In the second mode an external alarm triggered through a radio link is sounded if the appliance is disconnected from a power source. (See Bisak, col. 4, ll. 43-61). These two embodiments described in Bisak are not the same as the broadcasting beacon indicating stolen status as described in the present invention. In the present invention a beacon signal indicating that the item has been stolen is broadcast only if the receiver does not receive a valid key. "[A] wireless transmitter (2) for the equipment for broadcasting a beacon signal indicating stolen status, if the lock does not receive a valid key." (See Claim 1). This signal is designed to be received and read by others to inform them that the specific device has been stolen. In Bisak, if a valid key is not received, the unit sounds an audible alarm located on the appliance. This alarm is not a beacon designed to broadcast a signal if the appliance has been stolen. It is only an audible signal emitted from the appliance designed to inform someone that the appliance has been stolen. (See Bisak, col. 4, ll. 43-61). Thus, unlike Bisak, the present invention is not limited to broadcasting an alarm based solely on the appliance losing power. A beacon signal indicating stolen status can be broadcast based on an unauthorized user attempting to gain access to the device using the incorrect validation key. Applicants submit that an audible alarm sounded when the appliance is unplugged, the transmitter is unplugged, or the wrong code is received and an external alarm triggered through a radio link upon disconnecting power is not

the same as a wireless beacon signal indicating stolen status if the device does not receive a valid key.

Thus, it is respectfully submitted that Bisak does not disclose or suggest a "a wireless transmitter (20) for the equipment for broadcasting a beacon signal indicating stolen status, if the lock does not receive a valid key" as recited in claim 1. Accordingly, Applicants respectfully request that the Examiner should withdraw the 35 U.S.C. § 102(b) rejection of claim 1. Because claims 6-8, 10, 11, 14, 15, 19, 20, 22, and 23 depend from, and therefore, include all the limitations of claim 1, it is respectfully submitted that these claims are allowable for at least the reasons stated above.

Claim 18 recites a "a tamper detector (550) for detecting tampering with the system, and for permanently preventing use of the equipment if tampering is detected." The Examiner asserts that this recitation of claim 18 is disclosed in Bisak at column 4, lines 42-60 and column 5, lines 25-51. (See 4/5/07 Office Action, p. 3-4). Applicants respectfully disagree. Column 5, lines 25-51 from Bisak states,

> The control unit 37 is basically the same as the one for the transmitter-encoder. For example its main purpose is to provide communication between the receiver-decoder and the user, through the keyboard 39. The main difference is that the receiver-decoder cannot be turned off simply just by an on-off switch. If it could, it would not be secure at all. In this example the only way to turn the receiver-decoder off is by punching in the correct code on the keyboard 39, in which case the receiver-decoder will be deactivated and the appliance can be pulled out of the power socket and taken anywhere. However, when it is plugged back in the wall, a pulse is generated in the power supply (pulse generator 40) and that pulse turns the receiver-decoder on. Effectively the unit does not have to be turned on but does this itself automatically as soon as it is plugged in. This makes it a foolproof unit.
>
> The code within the receiver-decoder memory unit 31 is required to be the same as the one in the transmitter-decoder. If the two do not match, the alarm 32 will be activated. If the need arises to change the code in the memory 31, it can be changed through the keyboard 39. Naturally, it is inadequate if anyone can punch in a new code as a stolen appliance could be reused by someone else.

> The code can only be changed if one knows what the code in it already is.

However, Applicants submit that (1) an appliance not operating unless the correct code is received when the appliance is plugged in at a remote location from the transmitter from column 4, lines 42-60 and (2) the control unit as described in column 5, lines 25-51, are not the same as a tamper detection system that permanently prevents the use of the device if tampering is detected as described in claim 18.

Bisak describes a security device that renders an appliance inoperable unless the correct code is received. This security code is required whereupon the appliance has been plugged into a remote location from the transmitter. When the appliance is plugged in, the unit requires the correct code to be received from the transmitter before the unit becomes operable. (See Bisak, col. 4, ll. 43-50). Claim 18 recites a tamper detector that permanently prevents use of the equipment if any tampering is detected. In this system any tampering with the system, not limited to the device being moved, renders the system permanently inoperable. Upon any tampering condition the unit will cease to function, and cannot be reinitialized. This is different than the security device in Bisak that only renders the equipment inoperable when it has been moved, and only until the correct code has been entered. Applicants submit that a device that renders an appliance temporarily disabled until a correct code is entered, as described in Bisak, is not the same as a device that permanently prevents us of equipment upon the detection of any tampering, as described in claim 18.

Bisak also describes a code within a receiver-decoder memory unit. This code is matched with a code sent by the transmitter-decoder. If the code received by the receiver-decoder does not match the code transmitted by the transmitter-decoder, then an alarm is activated. This is different from a device that detects any tampering with the system, by an unauthorized user, and renders the device permanently inoperable upon detection of said tampering. (See Bisak, col. 54, ll. 26-51). In the claimed invention any tampering with the system, not limited to the device being moved, renders the system permanently inoperable. Upon any tampering condition the unit will cease to function, and cannot be reinitialized. This is different from the receiver-decoder in Bisak that only sounds an alarm if the incorrect security code has been received. Applicants submit that a receiver-decoder that enables an audible alarm

upon the receiving of an incorrect code, as described in Bisak, is not the same as a device that renders an appliance permanently disabled upon the detection of any tampering, as recited in claim 18.

Thus, it is respectfully submitted that Bisak does not disclose or suggest a "a tamper detector (550) for detecting tampering with the system, and for permanently preventing use of the equipment if tampering is detected" as recited in claim 18. Accordingly, Applicants respectfully request that the Examiner should withdraw the 35 U.S.C. § 102(b) rejection of claim 18.

## III. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

The Examiner has rejected claim 16 under 35 U.S.C. § 103(a) as unpatentable over Bisak in view of U.S. Patent No. 7,145,457 to Spitz et al. (hereinafter "Spitz").

The Examiner acknowledges that Bisak does not disclose that the identifier is traceable to an owner of the equipment. (See 04/05/07 Office Action p. 6).

Spitz is directed toward a method for information security access and to integrated visualization of information for an individual. The method provides for receiving data from various devices and normalizing said data based on uniquely identified objects. A programmed computer system receives the data from the devices and normalizes it to be easily accessible, and easily understandable, by security personnel. (See Spitz., col. 1, line 20 – col. 2, line 12).

Claim 16 recites an "an identifier, incorporated securely in the lock and traceable to an owner of the equipment in the case of theft of the equipment." The Examiner asserts that this recitation of claim 16 is disclosed in Spitz at column 16, line 49, to column 17, line 16. (See 4/5/07 Office Action, p. 6). Applicants respectfully disagree. Applicants submit that the log records containing information regarding, as an example, the office equipment being accessed and the user accessing it is different than the identifier incorporated securely in the lock as described in claim 16.

Spitz describes a system for centralizing security information to be easily accessed by security personnel. The system allows information such as employee information, office equipment information, and user security access to be stored centrally. This information can be used to determine employee access to particular areas within a building or particular equipment. Security can use this information to track where an employee has been and what equipment has been accessed. (See Spitz, col. 16, l. 49 – col. 17, l. 17). The invention of claim 16 does not compile various data regarding employee or equipment history or access. The invention of claim 16 involves a securely incorporated identifier to be located on the specific device being secured. This identifier contains information regarding the owner of the device. The system of claim 16 ,also does not involve a central location where all the information is stored. In Spitz when a user attempts to access a specific piece of equipment, the device contacts a central server to determine if the user has access to the equipment. In the present invention, the information is only stored locally. There is no communication between the security device and another location to determine the true owner of the device. Applicants submit that the centrally located log with employee information, user access, and office equipment information as described in Spitz is not the same as a local identifier located on the device being secured that only contains information regarding the true owner of the device.

Thus, it is respectfully submitted that Spitz does not disclose or suggest "an identifier, incorporated securely in the lock and traceable to an owner of the equipment in the case of theft of the equipment" as recited in claim 16. Accordingly, Applicants respectfully request that the Examiner should withdraw the 35 U.S.C. § 103(a) rejection of claim 16. Because claim 17 depends from, and therefore, includes all the limitations of claim 16, it is respectfully submitted that this claim is allowable for at least the reasons stated above.

The Examiner has rejected claim 24 under 35 U.S.C. § 103(a) as unpatentable over Bisak. Because claim 24 depends from, and, therefore includes all the limitations of claim 18, it is respectfully submitted that claim 24 is allowable at least for the reasons stated above with reference to claim 18.

The Examiner has rejected claims 2 and 21 under 35 U.S.C. § 103(a) as unpatentable over Bisak in view of U.S. Patent No. 6,975,202 to Rodriguez et al. (hereinafter "Rodriguez"). Because claim 2 depends from, and, therefore includes all the limitations of claim 1, it is respectfully submitted that claim 2 is allowable for the reasons stated above with reference to claim 1. Because claim 21 depends from, and, therefore includes all the limitations of claim 18, it is respectfully submitted that claim 21 is allowable at least for the reasons stated above with reference to claim 18.

The Examiner has rejected claims 3-5, 17 and 25 under 35 U.S.C. § 103(a) as unpatentable over Bisak in view of Spitz. Because claims 3-5 depend from, and, therefore include all the limitations of claim 1, it is respectfully submitted that claim 3-5 is allowable for the reasons stated above with reference to claim 1. Because claim 25 depends from, and, therefore includes all the limitations of claim 18, it is respectfully submitted that claim 25 is allowable at least for the reasons stated above with reference to claim 18.

The Examiner has rejected claim 12 under 35 U.S.C. § 103(a) as unpatentable over Bisak in view of U.S. Patent Publication No. 2003/0179078 to Chen et al. (hereinafter "Chen"). Because claim 12 depends from, and, therefore includes all the limitations of claim 1, it is respectfully submitted that claim 12 is allowable at least for the reasons stated above with reference to claim 1.

The Examiner has rejected claim 13 under 35 U.S.C. § 103(a) as unpatentable over Bisak in view of U.S. Patent No. 7,099,699 to Jeong. Because claim 13 depends from, and, therefore includes all the limitations of claim 1, it is respectfully submitted that claim 13 is allowable at least for the reasons stated above with reference to claim 1.

The Examiner has rejected claim 9 under 35 U.S.C. § 103(a) as unpatentable over Bisak in view of Spitz in further view of Rodriguez . Because claim 9 depends from, and, therefore includes all the limitations of claim 1, it is respectfully submitted that claim 9 is allowable at least for the reasons stated above with reference to claim 1.

## CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Please direct all future correspondence to:

Paul Im, Esq.
IP Counsel

Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9602
Fax: (914) 332-0615
Email: paul.im@philips.com

Respectfully submitted,

Dated: June 14, 2007

By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Phone: 212-619-6000
Fax: 212-619-0276